`UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

UNITED STATES OF AMERICA,	:	Case No. 3:10 CR 00522
Plaintiff,	:	JUDGE JAMES G. CARR
-vs-	:	
ALEX DAVID COOK,	:	**MOTION FOR NEW TRIAL**
Defendant.	:	(Evidentiary Hearing Requested)

Now comes the Defendant, Alex David Cook, by and through undersigned Counsel, and pursuant to Federal Criminal Rule 33, submits the following Motion for New Trial. An Evidentiary Hearing is requested on the Motion.

/s/Elizabeth Kelley
ELIZABETH KELLEY, 0063641
13940 Cedar Rd., #285
Cleveland, OH 44118-3204
(216)410-6923
ZealousAdvocacy@aol.com

SERVICE

I certify that on February 24, 2012, a copy of the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/Elizabeth Kelley
ELIZABETH KELLEY

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CIRCUIT CASES

UNITED STATES CONSTITUTION

FEDERAL RULES OF CRIMINAL PROCEDURE

I. INTRODUCTION

Alex David Cook was denied his constitutional right to due process, and ultimately, to a fair trial. The expert retained by first counsel failed to perform needed investigation and provide counsel with the information needed to properly represent Mr. Cook at trial. The expert retained by second counsel would have performed needed investigation; however, because the Court denied counsel her Motion to Continue Trial, that expert did not have sufficient time to perform that investigation. The failure to present an adequate defense resulted in actual prejudice, that is, Mr. Cook's conviction.

Mr. Cook now has compelling, documented, newly-discovered evidence showing that a third-party could have easily placed the illicit items on his computer. One juror has signed an affidavit stating that this information could have changed the verdict.

Therefore, in the interest of justice, Mr. Cook requests that the Court vacate his conviction and order a new trial.

II. STATEMENT OF THE CASE

On or about June 22, 2010, during an undercover session, Special Agent Richard Whisman, stationed with the FBI in Tulsa, Oklahoma, initiated a request through LimeWire to obtain child pornography. (Trial Transcript, p. 46). He obtained the requested items. In particular, there were several files offered from a user in Lima, Ohio. (Trial Transcript, p. 46). The Internet Protocol Address (IP address) showed that the service provider was Road Runner which is associated with Time Warner Cable. (Trial Transcript, p. 48).

Agent Whisman issued a subpeona to Time Warner. (Trial Transcript, p. 57-58). Records from Time Warner showed that the IP address in question was registered to an Alex David Cook of Lima, Ohio. (Trial Transcript, p. 59). Agent Whisman communicated with the FBI in the Northern District of Ohio and an investigation began. (Trial Transcript, p. 82).

FBI agents surveiled Mr. Cook's apartment five times before they executed a search. (Trial Transcript, p. 83, 85). They determined that he lived with another young man, Ian Douglas. (Trial Transcript, p. 84-85). On September 15, 2010, at approximately 7 a.m., a team of law enforcement entered Mr. Cook's apartment and executed a search warrant. (Trial Transcript, p. 86-88).

Mr. Cook was taken to the FBI office in the agents' car. (Trial Transcript, p. 88). At the FBI office, he was given a polygraph. At the grand jury held on December 8, 2010 and at the Suppression Hearing, the agent testified that the results were inconclusive. (Grand Jury Transcript, p. 13-14; Suppression Transcript, p. 70). (On August 24, 2011 and August 30, 2011, Mr. Cook took two polygraphs administered by

William D. Evans of Akron, Ohio. He passed both. *See* Exhibits A and B.) After that, Agent Pape testified that he took Mr. Cook's signed confession. (Trial Transcript, p. 140-41).

On November 12, 2010, Mr. Cook was arrested. He appeared before Magistrate Judge James Knepp, II, bond was set at $10,000 unsecured, and the Federal Public Defender's Office was assigned to represent Mr. Cook.

On December 8, 2010, Mr. Cook was indicted. He was charged with one count of knowingly distributing child pornography in violation of Title 18, United States Code, Section 2252A(a)(2)(A). On December 20, 2010, Mr. Cook was arraigned before Magistrate Knepp. Mr. Cook entered a not guilty plea and bond was continued.

On April 6, 2011, a Superceding Indictment was issued. Two additional charges were added: knowing receipt of child pornography in violation of Title 18, United States Code, Section 2256(2); and knowing possession of child pornography, in violation of Title 18, United States Code, Section 2252(a)(4)(B) . On April 11, 2011, Mr. Cook appeared before Judge James G. Carr, entered a plea of not guilty, and bond was continued.

On May 16, 2011, Mr. Cook filed a Motion to Suppress and a Motion in Limine. On July 6, 2011, a hearing on the Motion was held. On July 11, 2011, the Court issued a ruling stating that any statements made by Mr. Cook at and outside his apartment the morning of the search were suppressed. (Order, p. 9). However, statements during the session at the FBI office as well as the signed statement after the polygraph were admissible. (Order, p. 13).

On August 2, 2011, undersigned counsel filed a Notice of Appearance and Motion to Continue the Trial set for September 6, 2011. On August 4, 2011, the Court held a telephone conference. Counsel's Motion to Continue Trial was denied.

On September 6, 2011, a jury was empaneled and the trial began. At trial, Mr. Cook vehemently denied that he made a confession and instead, testified that the agent told him that he was drafting a letter to the U.S. Attorney recommending that the case be dismissed. The lack of any recording of this interrogation was of tremendous concern to the Court. (Trial transcript, p. 338-43; p. 433-36).

On September 9, 2011, the jury returned a guilty verdict as to all counts. The Court continued Mr. Cook's bond.

III. LAW

Federal Rule of Criminal Procedure 33 sets forth the grounds on which a Motion for New Trial may be based:

> (A) Defendant's Motion. Upon the defendant's motion, the court may vacate any judgement and grant a new trial if the interest of justice so requires. If the case was tried without a jury, the court may take additional testimony and enter a new judgement.
> (B) Time to File.
> (1) Newly Discovered Evidence. Any motion for a new trial grounded on newly discovered evidence must be filed within 3 years after the verdict or finding of guilty. If an appeal is pending, the court may not grant a motion for a new trial until the appellate court remands the case.
> (2) Other Grounds. Any motion for a new trial grounded on any reason other than newly discovered evidence must be filed within 14 days after the verdict or finding of guilty.

The factors for granting a new trial motion are as follows:

> In order to prevail on a Rule 33 motion for a new trial, a defendant must show the following: "(1) the new evidence was discovered after the trial; (2) the evidence could not have been discovered earlier with due diligence; (3) the evidence is material and not merely cumulative or impeaching; and (4) the evidence would likely produce acquittal." United States v. Carson, 560 F.3d 566, 585 (6th Cir. 2009)(*quoting* United States v. Seago, 930 F.2d 482, 488 (6th Cir. 1991)).

For the reasons which follow, Mr. Cook respectfully submits that it is in the interest of justice to vacate his conviction and order a new trial based on newly-discovered evidence.

IV. ARGUMENT

ALEX COOK WAS DENIED HIS CONSTITUTIONAL RIGHT TO DUE PROCESS AS GUARANTEED BY THE FIFTH AMENDMENT TO THE UNITED STATES CONSTITUTION BECAUSE OF A LACK OF AN OPPORTUNITY TO PRESENT AN ADEQUATE DEFENSE.

A review of the record will show that prior to his indictment, other than traffic offenses, Mr. Cook had never been in trouble with the law. Indeed, he was a 19-year old man, an Eagle Scout, and came from a stable, loving two-parent family in Knox County, Ohio. Thus, as undersigned Counsel pointed out at the telephone conference held on August 4, 2011 wherein the Court denied her Motion to Continue the Trial, the family was unfamiliar with the daunting aspects of a criminal case, believed in their son's innocence, and wanted a trial. Moreover, the fact that they retained counsel on the eve of trial was not an attempt to delay and game the system, but rather, they did not know that they could hire someone other than a public defender, and once they learned this, they wanted to do so in a methodical fashion. (Telephone Conference Transcript, p. 17-18).

In her Motion for a Continuance, counsel noted that the case file was voluminous. And during the telephone conference, she also noted the need to retain a new computer forensic expert. (Telephone Conference Transcript, p. 10, 18). Although the Government estimated that would be a two-day trial, it ended up lasting four days. (Telephone Conference Transcript, 3, 10).

Bill Jonke, a trial consultant retained by the family following the verdict, interviewed several jurors. They based their decision on two factors: "that the exhibits in question were in fact found upon his [Mr. Cook's] computer" and that he confessed to Agent Pape. *See* affidavit marked as Exhibit C.

Thus, the presence of the images was a huge concern to the jury. Unfortunately, neither counsel could explain the source of the images. The expert retained by the federal public defender made no effort to explain the source notwithstanding the fact that he had several months to explore this issue. Indeed, as the affidavit from Mr. Jonke notes, that expert, Wayne Marney, never investigated the issue of third-party planting nor did he advise counsel of this possibility. Moreover, the affidavit from Mr. Jonke notes that Mr. Marney became most unpleasant when Mr. Jonke raised this possibility.

Accordingly, when undersigned counsel stepped into the shoes of prior counsel, she inherited a report which was not helpful to her client. With a month before trial, she contacted Mark Vassel, a computer forensic expert whom she has used in the past, and requested that he examine Mr. Cook's hard drive, prepare a report, and be available to testify at trial. *See* affidavit from Mark Vassel marked as Exhibit D. Mr. Vassel accommodated that request. However, as his affidavit notes:

> 7. Never in my conversations with Attorney Kelley did I raise the possibility that a third party might have remotely planted the child pornography on Mr. Cook's computer. Indeed, to perform such an analysis, I would have needed at least ninety (90) days. *Because of the short time which the Court gave her to prepare for trial, this would have been impossible*. (Emphasis added.)

Now, with the lapse of several months since Mr. Cook's conviction, undersigned counsel, with the assistance of Mr. Jonke, has been able to explore the issue of third-party access.

The attached presentation assembled by Carl Herkimer, a self-described computer hacker, shows that anyone with a knowledge of computers can place images on someone else's computer without their knowledge. (A copy of the presentation is attached to this Motion via the Court's electronic filing system. Admittedly, this attachment is blurry

because of transmission. Thus, thumb drives with this presentation will be hand-delivered to the Court and to the U.S. Attorney's Office. Additional copies will be available on request.)

The presentation shows the ability of a person's or "hacker's" gaining access to another's computer across a wireless internet connection. This access gives the hacker complete and total control of the computer he/she accesses without the victim's knowing that his/her computer has been compromised.

Once a hacker is able to receive a wireless signal, he/she can run an application that will search the network and automatically determine and provide the hacker with any wireless router and/or computer's encryption and passwords. There are numerous types of these applications available as "Freeware" (no charge) on the internet. Here, the application being used is called Cain and Abel. As with most software, this application was intended as a beneficial application. Yet in the wrong hands, it is destructive. As demonstrated, within a matter of seconds, the application has discovered and provided the wireless encryption key and computer password. Once the hacker has this information, the remote computer is completely vulnerable.

The other application used for this presentation was P2P (Peer to Peer), a software application called LimeWire. Indeed, there are many types of P2P applications available as Freeware on the internet. This P2P or computer-to-computer allows "sharing," or in this case, "parking" or placing of files on someone's computer without his/her knowledge.

Below is a step-by-step outline of this process as shown in the presentation. It shows how files can be placed on a victim's computer without his/her knowledge:

Step 1: Hacker discovers wireless network and runs the Cain and Abel software to learn password;

Step 2: After applying the password, the hacker has complete, unfettered access to the victim's computer. The hacker can place any type of file on the victim's computer and place these files deep within the file structure to keep them from being discovered. As seen in the presentation, the hacker is going deep within the computer's file system to the LimeWire directory and further into the LimeWire "Saved" sub-folder where there are no files, at this point.

Step 3: The hacker then goes to his/her "BadGuy" computer and he/she can now see the victim's entire computer.

Step 4: The hacker simply copies, or drags and drops files from his/her computer or the internet to the victim's computer for later retrieval.

Step 5: The hacker can return to the victim's computer and verify that the files are there.

Step 6: The presentation shows the files on the victim's computer. The presentation also shows that the file names can be altered so they are misleading as to their content. One cannot determine what is in the file merely by its name. The file must first be discovered and then it must be opened to see what it actually is. If it were never opened, the victim would not know it was there. Additionally, if the victim does not have a complete file, as was the case here with several files, one cannot make assumptions about its content.

Third-party planting becomes even easier if the third-party knows the password of the victim's computer. As the affidavit from Mr. Jonke notes, Mr. Cook shared his password with at least two individuals. Moreover, because Mr. Cook's router was in his

window, his router had a range of more than one hundred yards, and the parking lot was only a few yards from that window, anyone could have accessed his computer.

Had Counsel been allowed time to fully explore the issue of third-party planting and to make a presentation such as this to the jury, it could have made a difference in the verdict. *See* attached affidavit from William Rexer, one of the jurors.

Indeed, the issue of third-party planting was of concern to the grand jury. At the grand jury proceeding held on December 8, 2010, one juror asked:

> I understand that you can download with files from somebody else's computer, can you also push data to somebody with the same software?
> THE WITNESS [Agent Schulte]: Not that I'm aware of. Anything that you get from LimeWire you need to initiate the download. Now you may not always know what you're getting –
> JUROR: Right.
> THE WITNESS: – you could think you're downloading a song and get a virus *but you need to initiate a download for something to end up on your computer.* (p. 13-14. Emphasis added.)

The fact that the agent testified that third-party cannot "push" data onto another's computer is significant, and is directly refuted by the attached presentation.

Furthermore, at trial, during cross-examination, Detective Morford testified to the same:

> A. *Nobody on Gnutella can push a file up to your computer.* Somebody in that local network could put something behind that router if it was shared and opened for them to do that.
> Q: But you needn't necessarily know that person, would you?
> A: If they're accessing your network, I would think you would know who's on your network. (Trial Transcript, p. 253. Emphasis added.)

Additionally, an affidavit from Kathryn Koch, a licensed private investigator in Columbus shows that this was done to her.

At trial, Alex himself testified that he came home one afternoon and inexplicably found two images which he promptly deleted. (Trial Transcript, p. 303-05). This was confirmed by Mr. Vassel's examination (Trial Transcript, p. 350-51), relayed at trial by Dr. Wayne Graves, a forensic psychologist who interviewed Alex. (Trial Transcipt, p. 203).

The aforementioned newly-discovered evidence meets the factors set forth in Carson and Seago for granting a new trial.

1. The attached demonstration of third-party planting was assembled after trial. With the benefit of time, counsel was able to fully explore all alternate theories as to how the illicit images appeared on Mr. Cook's computer. (Because of the short time to prepare for trial, counsel tried to cast suspicion on the logical alternate source, the roommate, Ian Douglas. The jury clearly rejected that theory.) Finally, Mr. Herkimer was located and his demonstration shows how easy third-party planting is.

2. The evidence could not have been discovered earlier without due diligence. Given the shortcomings of the first forensic expert and given the severe time constraints placed on the second forensic expert, this evidence could not have been developed. First counsel was as diligent as she could have been, but her ability to fully represent Mr. Cook was hampered by an expert who did not properly advise her. Second counsel had a highly-competent expert who advised her as completely as he could, but he had only a month, and because of her urgent request that he review the discovery, conduct an examination, prepare a report, and make himself available to testify within a month, his response was to fill that request and not emphasize the need for additional time. In short,

it could not have been discovered because neither counsel did not know what she did not know.

3. The newly-discovered evidence is material, and not merely cumulative or impeaching.

In this Motion, Mr. Cook is not attempting to re-litigate the trial. The evidence of third-party planting is entirely new. Indeed, two of the Government's witnesses denied its existence, once before the grand jury and the other at trial. And as one juror noted, it could have changed his vote.

4. The newly-discovered evidence is likely to produce an acquittal.

The jury deliberated for approximately four hours. As the affidavit from Mr. Jonke notes, the jurors were greatly impacted by this case. They took their responsibility seriously. Demonstrating to them just how easy it is to plant images on someone else's computer may very well have shown them that although these images, indisputably, were on Mr. Cook's computer, he did not have knowing possession, knowing receipt, and did not knowingly distribute them. In other words, this would have planted reasonable doubt in the minds of the jurors.

Therefore, in the interests of justice, for the foregoing reasons, Alex Cook requests that this Honorable Court grant him an evidentiary hearing, and ultimately, grant this Motion for a New Trial.

Respectfully submitted,

/s/Elizabeth Kelley
Counsel for Mr. Cook